UBND TỈNH KHÁNH HÒA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 457 /STTTT-CNTTBCVT

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2023

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Khánh Hòa, ngày 22 tháng 02 năm 2023

Kính gửi:
- Các cơ quan Đảng, Mặt trận, đoàn thể tỉnh;
- Các sở, ban, ngành;
- UBND các huyện, thị xã, thành phố;
- Các đơn vị sự nghiệp trực thuộc UBND tỉnh.

Sở Thông tin và Truyền thông nhận được Công văn số 158/CATTT-NCSC ngày 15/02/2023 của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2023.

Theo nội dung Công văn số 158/CATTT-NCSC ngày 15/02/2023, Microsoft đã phát hành danh sách bản vá tháng 02 với 75 lỗ hổng bảo mật trong các sản phẩm của mình, trong đó, đáng chú ý là các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng sau:

- 04 lỗ hổng bảo mật **CVE-2023-21529, CVE-2023-21710, CVE-2023-21707, CVE-2023-21706** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. Microsoft Exchange Server đã và đang là mục tiêu hàng đầu được các nhóm tấn công có chủ đích (APT) nhắm đến, các đối tượng tấn công khai thác triệt để. Vì vậy, các cơ quan, tổ chức cần đặc biệt chú ý cũng như có kế hoạch để khắc phục và tăng cường giám sát nhằm giảm thiểu và tránh nguy cơ bị tấn công thông qua các lỗ hổng này.

- Lỗ hổng bảo mật **CVE-2023-21716** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-21715** trong Microsoft Publisher cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế.

- 02 lỗ hổng bảo mật **CVE-2023-23376, CVE-2023-21812** trong Windows Common Log File System (CLFS) cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- 03 lỗ hổng bảo mật **CVE-2023-21705, CVE-2023-21713, CVE-2023-21528** trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-21717** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

Việc khai thác thành công lỗ hổng nêu trên có thể cho phép đối tượng thực thi mã từ xa, tấn công nâng cao đặc quyền trong hệ thống mục tiêu, từ đó có thể chiếm quyền điều khiển toàn bộ hệ thống.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị, địa phương, Sở Thông tin và Truyền thông đề nghị Quý cơ quan thực hiện các nội dung sau:

1. Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng; thực hiện cập nhật bản vá bảo mật cho các máy có nguy cơ bị tấn công theo hướng dẫn của Microsoft tại Phụ lục kèm theo Công văn số 158/CATTT-NCSC (*gửi kèm Công văn này*).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Khẩn trương thông báo nội dung văn bản này đến tất cả các cơ quan, đơn vị trực thuộc để tổ chức triển khai thực hiện.

Quá trình thực hiện nếu có vướng mắc, đề nghị Quý cơ quan liên hệ đầu mối thường trực Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (điện thoại: 0258.3563533 - thư điện tử: cnttbcvt.stttt@khanhhoa.gov.vn) để được hướng dẫn, hỗ trợ.

Sở Thông tin và Truyền thông thông báo và đề nghị Quý cơ quan, đơn vị, địa phương quan tâm thực hiện.

Trân trọng./.

Nơi nhận:
- Như trên (VBĐT);
- Các phòng, đơn vị thuộc Sở (VBĐT, để t/h);
- Lưu: VT, CNTTBCVT (KD, 02).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH KHÁNH HÒA

Nguyễn Văn Hiền